HKUST – Department of Computer Science and Engineering
COMP 2711: Discrete Math Tools for CS – Fall 2015

Serial #

Final Examination

Date: Monday, 14 December 2015 Time: 8:30am – 11:30am

Name: _____	Student ID: _____
Email: _____	Lecture Section: _____
Program: _____	

Instructions:

- **Read the following instructions carefully before working on the problems**.
- This is a closed book exam. One cheat sheet written on double-sided A4 paper is allowed.
- The exam consists of 10 questions and 19 pages.
- Please write your name, student ID, email, lecture section and program on this page. For each subsequent page, please write your student ID at the top of the page in the space provided.
- Please sign the honor code statement on page 2.
- Answer all the questions within the space provided on the examination paper. *You may use the back of the pages for your answers or rough work.* The last **two** pages are scrap papers and can be torn off.
- Unless otherwise specified you *must* always explain how your answers are derived. A number without an explanation will be considered an incorrect answer.
- *Ask an invigilator for clarification if you feel there is any ambiguity with any of the problems.*

Questions	1	2	3	4	5	6	7	8	9	10	Total
Score											

Student ID: _____

As part of HKUST's introduction of an honor code, the HKUST Senate has recommended that all students be asked to sign a brief declaration printed on examination answer books that their answers are their own work, and that they are aware of the regulations relating to academic integrity. Following this, please read and sign the declaration below.

I declare that the answers submitted for this examination are my own work.

I understand that sanctions will be imposed, if I am found to have violated the University regulations governing academic integrity.

Student's Name: _____

Student's Signature: _____

Student ID: _____

Problem 1: [10 pts]
Consider rolling two fair dice and let D_1 and D_2 be the results respectively. Define $X = \max\{D_1, D_2\}$. In other words, X is the maximum of D_1 and D_2.

(a) What is the distribution function of the random variable X? Show how your answer is derived.

(b) What is the expectation $E(X)$ of X? Show how your answer is derived.

(c) What is the variance $V(X)$ of X? Show how your answer is derived.

(d) Let Y be the maximum of the results of rolling three fair dice. Is $V(Y)$ larger or smaller than $V(X)$? Give an intuitive explanation. There is no need to do any calculations for this part.

[MORE WORKSPACE ON NEXT PAGE]

Student ID: _____

[ADDITIONAL WORKSPACE FOR PROBLEM 1]

Solution: (a) Consider a value k of X, with $1 \leq k \leq 6$. We have

$$\begin{aligned} P(X=k) &= P(D_1=k, D_2=k) + P(D_1=k, D_2<k) + P(D_1<k, D_2=k) \\ &= P(D_1=k)P(D_2=k) + P(D_1=k)P(D_2<k) + P(D_1<k)P(D_2=k) \\ &= \frac{1}{36} + (\frac{1}{6})(\frac{k-1}{6}) + (\frac{k-1}{6})(\frac{1}{6}) \\ &= \frac{2k-1}{36} \end{aligned}$$

Consequently,

k	1	2	3	4	5	6
$P(X=k)$	$\frac{1}{36}$	$\frac{3}{36}$	$\frac{5}{36}$	$\frac{7}{36}$	$\frac{9}{36}$	$\frac{11}{36}$

(b) By the definition of expectation, we have

$$\begin{aligned} E(X) &= 1 \times \frac{1}{36} + 2 \times \frac{3}{36} + 3 \times \frac{5}{36} + 4 \times \frac{7}{36} + 5 \times \frac{9}{36} + 6 \times \frac{11}{36} \\ &= \frac{161}{36} \approx 4.47 \end{aligned}$$

(c) By the definition of variance, we have

$$\begin{aligned} V(X) &= (1-\frac{161}{36})^2 \times \frac{1}{36} + (2-\frac{161}{36})^2 \times \frac{3}{36} + (3-\frac{161}{36})^2 \times \frac{5}{36} + (4-\frac{161}{36})^2 \times \frac{7}{36} + \\ &\quad (5-\frac{161}{36})^2 \times \frac{9}{36} + (6-\frac{161}{36})^2 \times \frac{11}{36} \\ &\approx 1.97 \end{aligned}$$

(d) $V(Y)$ is smaller than $V(X)$. In comparison with the distribution of D_1 (or D_2), the distribution of X concentrates more to the right, resulting in a smaller variance ($V(D_1) \approx 2.9$). The distribution of Y concentrates even more to the right, leading to a even smaller variance.

Grading: 3, 2, 2, 3

Student ID: _____

Problem 2: [8 pts]

For this problem, the time is discretized into equal-sized intervals and the length of each interval is 1 minute.

An online store sells bags. At each time interval, the probability of one customer arriving is p, and the probability of no customer arriving is $1-p$. Each customer buys one bag with probability q and does not buy anything with probability $1-q$.

For simplicity, assume that each customer arrives at the store, completes purchase, if any, and leaves the store within the same 1-minute time interval.

Let X be the total number of bags sold within 60 minutes.

(a) What is the range of X? That is, what are the possible values with non-zero probabilities?

(b) For a possible value k of X, what is $P(X = k)$?

(c) What is the expectation $E(X)$ of X?

(d) What is the variance $V(X)$ of X?

There is no need to justify your answers in this problem.

[MORE WORKSPACE ON NEXT PAGE]

Solution :

This is an independent Bernoulli trials process with success probability pq.

(a) The range of X is $\{0, 1, \ldots, 60\}$

(b) X follows the binomial distribution. The probability $P(X = k)$ of exactly k successes:

$$P(X = k) = \binom{60}{k}(pq)^k(1-pq)^{60-k}.$$

(c) $E(X) = 60pq$.

(d) $V(X) = 60pq(1-pq)$.

Grading: 2, 2, 2, 2

[ADDITIONAL WORKSPACE FOR PROBLEM 2]

Student ID: _____

Problem 3: [10 pts]
Continuing with the previous problem, suppose that the store sells n brands of bags, where $n > 1$, and each bag purchased can be any of the n brands with equal probability, i.e., $\frac{1}{n}$.

Assume all brands are marked white at the beginning of a 60 minute period. A brand is marked red once a bag of the brand is sold, and remains that way in the rest of the time period.

(a) What is the expected number of brands that are marked red within the 60 minute period?

(b) What is the probability that all brands are marked red within the 60 minute period?

Give your answers as mathematical expressions in terms of p, q and n. Explain how your answers are derived.

[MORE WORKSPACE ON NEXT PAGE]

Solution : (a) Let us first calculate the probability that a given brand i is marked red within 60 minutes.

$$\begin{aligned} & P(\text{Brand } i \text{ marked red within 60 minutes}) \\ = \; & P(\text{At least one bag of Brand } i \text{ sold within 60 minutes}) \\ = \; & 1 - P(\text{No bags of Brand } i \text{ sold within 60 minutes}) \\ = \; & 1 - P(\text{No bags of Brand } i \text{ sold within 1st minute}) \\ & \quad P(\text{No bags of Brand } i \text{ sold within 2nd minute}) \\ & \quad \cdots \\ = \; & 1 - (1 - \frac{pq}{n})^{60} \end{aligned}$$

Let X_i be the indicator random variable that takes value 1 if Brand i is marked red within the 60 minute minute, and 0 otherwise. Then

$$E(X_i) = 1 - (1 - \frac{pq}{n})^{60}.$$

Further let X be the number of brands marked red within the 60 minute period. Then $X = \sum_{i=1}^{n} X_n$. By the linearity of expectation, we have

$$E(X) = \sum_{i=1}^{n} E(X_n) = n(1 - (1 - \frac{pq}{n})^{60}).$$

Student ID: _____

[ADDITIONAL WORKSPACE FOR PROBLEM 3]

Solution : (b) Let E_i be the event that Brand i is not marked red during the 60 minute period. We have,

$$\begin{aligned} & P(\text{All brands are marked red within the 60 minute period}) \\ = \; & 1 - P(\cup_{i=1}^{n} E_i) \end{aligned}$$

By the Inclusion-Exclusion principle, we have

$$\begin{aligned} P(\cup_{i=1}^{n} E_i) &= \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \le i_1 < i_2 < \ldots < i_k} P(E_{i_1} \cap E_{i_2} \cap \ldots \cap E_{i_k}) \\ &= \sum_{k=1}^{n} (-1)^{k+1} \binom{n}{k} (1 - pq\frac{k}{n})^{60} \end{aligned}$$

Therefore,

$$\begin{aligned} & P(\text{All brands are marked red within the 60 minute period}) \\ = \; & 1 - \sum_{k=1}^{n} (-1)^{k+1} \binom{n}{k} (1 - pq\frac{k}{n})^{60}. \end{aligned}$$

Grading: 5, 5

Student ID: _____

Problem 4: [8 pts]
Continuing with the previous problem, suppose the store was taken offline for maintenance and has just been put back online.

(a) What is the expected number of minutes until the first bag is sold (or, equivalently, until the first brand is marked red)?

(b) What is the expected number of minutes until all brands are marked red?

Justify your answers.

Solution :

(a) For this part, we have an independent Bernoulli trials process with success probability pq. The expected time until the first success is $\frac{1}{pq}$ minutes.

(b) For this part, we deal with a multiple-stage Bernoulli trials process. The first stage starts from the beginning and ends when the first brand is marked red. In this stage the success probability of each trial is pq. The expected length of the stage is $\frac{1}{pq}$.
The second stage starts after the first brand is marked and ends when the second brand is marked red. In this stage the success probability of each trial is $pq\frac{n-1}{n}$. The expected length of the stage is $\frac{n}{pq(n-1)}$.
Similarly, the expected length of the third stage is $\frac{n}{pq(n-2)}$, and the expected length of the last (n-th) stage is $\frac{n}{pq(n-(n-1)}$.
Hence, the expected number of minutes until all brands are marked red is

$$\sum_{i=1}^{n} \frac{n}{pq(n-i+1)} = \frac{n}{pq}\sum_{i=1}^{n} \frac{1}{n-i+1} = \frac{n}{pq}\sum_{i=1}^{n} \frac{1}{i}.$$

Grading: 3, 5

Student ID: _____

Problem 5: [10 points]
Let p be a prime number. For any two integers x and y from Z_p, if

$$x = y^2 \bmod p,$$

then we say that x is a *quadratic residue mod* p, and that y is a *square root of* x *mod* p.

(a) Find all integers in Z_{11} that are quadratic residues mod 11.

(b) Show that $p - 1$ is a square root of 1 mod p.

(c) Show that if y is a square root of x mod p, so is $p - y$.

Solution: (a) $0(y = 0), 1(y = 1, 10), 3(y = 5, 6), 4(y = 2, 9), 5(y = 4, 7), 9(y = 3, 8)$.
(Note on grading: Only the value of x is required.)

(b) $(p-1)^2 \bmod p = (p^2 - 2p + 1) \bmod p = 1 \bmod p = 1$

(c) $(p-y)^2 \bmod p = (p^2 - 2py + y^2) \bmod p = y^2 \bmod p = x$

Grading: 4, 3, 3

Student ID: _____

Problem 6: [14 points] Assume for the RSA scheme, you are given p=17 and q=31.

(a) Which *one* of the following integers can be used as the public key e: 2, 5 or 7? Explain. (Note: There is only one possible choice.)

(b) Find the private key d using the extended GCD algorithm for the public key e picked at Part (a). Show all steps of your calculations.

(c) Suppose the ciphertext is 2. Decrypt it to find the plaintext. Show all steps of your calculations.
You may find the following equalities helpful: $171^2 \bmod 527 = 256$, $256^2 \bmod 527 = 188$, $35 \times 171 \bmod 527 = 188$, and $188^2 \bmod 527 = 35$.

[MORE SPACE ON NEXT PAGE]

Solution:

(a) p=17, q=31, so T=(17-1)*(31-1)=16*30, only 7 is relatively prime to T, we will be able to find the inverse only for 7, therefore e=7

(b) We use the extended GCD algorithm to find the d which is the inverse of e in modulo T, $T=(p-1)(q-1) = 480$. First we find the greatest common divisor of T and e

$$\begin{aligned} 480 &= 7 \times 68 + 4 \\ 7 &= 4 \times 1 + 3 \\ 4 &= 3 \times 1 + 1 \\ 3 &= 1 \times 3 + 0 \end{aligned}$$

Therefore gcd(480,7)=1. Now we roll back to get the inverse of 7

$$\begin{aligned} 1 &= 1 \times 1 + 3 \times 0 \\ &= 4 - 3 \\ &= 4 - (7 - 4 \times 1) \\ &= 4 \times 2 - 7 \\ &= (480 - 7 \times 68) \times 2 - 7 \\ &= 480 \times 2 + 7 \times (-137) \end{aligned}$$

Therefore $d = -137 \bmod 480 = 343$.

[ADDITIONAL WORKSPACE FOR PROBLEM 6]

(c) To decrypt the ciphertext 2, we need to do the following:

$$2^{343} \bmod (17 \times 31)$$
$$2^{343} \bmod 527$$

Since $343 = 101010111_{(2)}$ (i.e., $343 = 2^8 + 2^6 + 2^4 + 2^2 + 2 + 1$), we need to get I_0, I_1,I_2,I_4, I_6 and I_8:

$$\begin{array}{lll} I_0 & 2 \; mod \; 527 & = 2 \\ I_1 & I_0 \times I_0 \bmod 527 & = 4 \\ I_2 & I_1 \times I_1 \bmod 527 & = 16 \\ I_3 & I_2 \times I_2 \bmod 527 & = 256 \\ I_4 & I_3 \times I_3 \bmod 527 & = 188 \; (given) \\ I_5 & I_4 \times I_4 \bmod 527 & = 35 \; (given) \\ I_6 & I_5 \times I_5 \bmod 527 & = 171 \\ I_7 & I_6 \times I_6 \bmod 527 & = 256 \; (given) \\ I_8 & I_7 \times I_7 \bmod 527 & = 188 \; (given) \end{array}$$

Now we have:

$$\begin{aligned} 2^{343} \bmod 527 &= (I_8 \times I_6 \times I_4 \times I_2 \times I_1 \times I_0) \bmod 527) \\ &= (188 \times 171 \times 188 \times 16 \times 4 \times 2) \bmod 527 \\ &= ((188^2 \bmod 527) \times 171 \times 16 \times 4 \times 2) \bmod 527 \\ &= ((35 \times 171 \bmod 527) \times 16 \times 4 \times 2) \bmod 527 (given) \\ &= (188 \times 16 \times 4 \times 2) \bmod 527 \; (given) \\ &= 24064 \bmod 527 \\ &= 349 \end{aligned}$$

Therefore the plaintext is 349.

Grading: 3, 5, 6

Student ID: _____

Problem 7: [10 points]

(a) Use Fermat's Little Theorem and the Chinese Reminder Theorem to show that, if an integer a is not divisible by any of 3, 5 and 7, then

$$a^{49} \bmod 105 = a \bmod 105.$$

(b) Use Part (a) to calculate

$$4^{385} \bmod 105.$$

Solution:

(a) Note that $105 = 3 \times 5 \times 7$. We also have:
$a^{49} \bmod 3 = (a^{24*(3-1)+1}) \bmod 3 = a \bmod 3$ by FLT
$a^{49} \bmod 5 = (a^{12*(5-1)+1}) \bmod 5 = a \bmod 5$ by FLT
$a^{49} \bmod 7 = (a^{8*(7-1)+1}) \bmod 7 = a \bmod 7$ by FLT
By CRT, we have

$$a^{49} \bmod 3 \times 5 = a \bmod 15.$$

Applying CRT again we get

$$a^{49} \bmod 15 \times 7 = a \bmod 105.$$

(b) By the result of (a)

$$\begin{aligned} 4^{385} \bmod 105 &= 4^{(7*49)+42} \bmod 105 \\ &= ((4^{7*49} \bmod 105) \times 4^{42}) \bmod 105 \\ &= ((4^7 \times 4^{42}) \bmod 105 \\ &= 4^{49} \bmod 105 = 4 \bmod 105 = 4. \end{aligned}$$

Grading: 6, 4

Student ID: _____

Problem 8: [10 pts]

(a) Consider the recurrence below defined for $n \geq 0$.

$$T(n) = \begin{cases} 3 & \text{if } n = 0 \\ 7T(n-1) + 12 & \text{if } n > 0 \end{cases}$$

Give a closed-form solution to the recurrence. You only have to give the solution. You do **not** need to show how you derived it.

(b) Prove the correctness of your solution by **induction**.

Solution: (a) By iterating the recurrence, we get:

$$T(n) = 3 \cdot 7^n + 12 \cdot \frac{7^n - 1}{7 - 1} = 5 \cdot 7^n - 2.$$

(b) We need to prove:

$$T(n) = 5 \cdot 7^n - 2 \tag{1}$$

Base case: When $n = 0$, $T(0) = 3 = 5 \cdot 7^0 - 2$. Equation (1) is true.
Inductive step: Now consider $n > 1$. Assume Equation (1) is true for the case of $n - 1$, i.e.,

$$T(n-1) = 5 \cdot 7^{n-1} - 2.$$

For the case of n, we have

$$\begin{aligned} T(n) &= 7T(n-1) + 12 \\ &= 7(5 \cdot 7^{n-1} - 2) + 12 \qquad \text{(induction hypothesis)} \\ &= 5 \cdot 7^n - 2. \end{aligned}$$

By the weak principle of mathematical induction, we conclude that Equation (1) is true for all $n \geq 0$.

Grading: 4, 6

Student ID: _____

Problem 9: [10 pts]

Let A and B be two positive integers represented as binary sequences, each n bits long. Assume n is a power of 2. The product $A \cdot B$ can be computed recursively as follows:

1. If $n = 1$, calculate $A \cdot B$ directly.
2. If $n > 1$, partition the bit representation of each number into two parts, the high $\frac{n}{2}$ bits and low $\frac{n}{2}$ bits. Calculate $A \cdot B$ using the following formula:

$$\begin{aligned} & A \cdot B \\ = \; & (A_h \cdot 1\underbrace{0\ldots0}_{n/2} + A_l) \cdot (B_h \cdot 1\underbrace{0\ldots0}_{n/2} + B_l) \\ = \; & (A_h \cdot B_h) \cdot 1\underbrace{0\ldots0}_{n} + (A_h \cdot B_l) \cdot 1\underbrace{0\ldots0}_{n/2} \\ & + (A_l \cdot B_h) \cdot 1\underbrace{0\ldots0}_{n/2} + (A_l \cdot B_l) \end{aligned} \tag{2}$$

   where A_h and B_h denote the high $\frac{n}{2}$ bits of A and B, respectively, and A_l and B_l denote the low $\frac{n}{2}$ bits of A and B, respectively. The terms in ( ) are calculated recursively.

Suppose the calculations take 1 unit of time when $n = 1$, and suppose that calculation of the expression (2) takes cn units of time given the results of the recursive calls, where c is a constant.

Let $T(n)$ be the total time it takes to compute $A \cdot B$. Write a recurrence for $T(n)$, find a closed-form expression for it, and simplify the closed-form expression using the big Θ notation.

[MORE SPACE ON NEXT PAGE]

[ADDITIONAL WORKSPACE FOR PROBLEM 9]

Solution: According to the above expression of $A \cdot B$,

$$T(n) = 4T(\tfrac{n}{2}) + cn$$

Iterating the recurrence, we get:

$$\begin{aligned}
T(n) &= T(2^j) \\
&= 4T(2^{j-1}) + 2^j c \\
&= 4(4T(2^{j-2}) + 2^{j-1}c) + 2^j c \\
&= 4^2 T(2^{j-2}) + 2 \cdot 2^j c + 2^j c \\
&= 4^2(4T(2^{j-3}) + 2^{j-2}c) + 2 \cdot 2^j c + 2^j c \\
&= 4^3 T(2^{j-3}) + 2^2 \cdot 2^j c + 2 \cdot 2^j c + 2^j c \\
&\vdots \\
&= 4^j T(1) + 2^{j-1} \cdot 2^j c + \ldots + 2 \cdot 2^j c + 2^j c \\
&= 4^j + 2^j c(2^j - 1) \\
&= (1+c)n^2 - cn \\
&= \Theta(n^2)
\end{aligned}$$

Grading: Recurrence 3, iterating recurrence 5, big theta 2

Student ID: _____

Problem 10: [10 pts] Prove the following statement by induction

$$\Big(n(n-1)\cdots(2)(1)+1\Big) \bmod m = 1$$

for all integer $n > 1$ and for any $m \in \{2, 3, \cdots, n\}$.

Note: No marks will be awarded if you do not use the principle of induction.

Solution: Let $p(n)$ denotes $\Big(n(n-1)\cdots(2)(1)+1\Big) \bmod m = 1$.
Base case ($n = 2$): $(2+1) \bmod 2 = 1$, so $p(2)$ is true.
Inductive hypothesis: Assume $p(n-1)$ is true for $n - 1 > 1$.

$$\Big((n-1)\cdots(2)(1)+1\Big) \bmod m = 1$$

Inductive step (for $n > 2$):

$$\begin{aligned}
& \Big((n-1)\cdots(2)(1)+1\Big) \bmod m = 1 \\
\rightarrow\ & \Big(n(n-1)\cdots(2)(1)+n\Big) \bmod m = n \bmod m \\
\rightarrow\ & \Big(n(n-1)\cdots(2)(1)+1+(n-1)\Big) \bmod m = n \bmod m \\
\rightarrow\ & \Big(n(n-1)\cdots(2)(1)+1\Big) \bmod m = (n-(n-1)) \bmod m \\
\rightarrow\ & \Big(n(n-1)\cdots(2)(1)+1\Big) \bmod m = 1
\end{aligned}$$

Inductive conclusion: By the principle of mathematical induction, $p(n)$ is true for all integers $n > 1$.

Grading: Framework of proof 5, concrete reasoning 5